IN THE CLAIMS:

A status of all the claims of the present Application is presented below:

1. **(Original)** A computer comprising:

an operating system controlling a computer resource; and

an intrusion detection system integrated with the operating system and operable to monitor the computer resources to detect and prevent intrusion attempts.

2. **(Original)** The computer, as set forth in claim 1, wherein the computer resource is selected from the group consisting of data storage system, input/output system, a networking system, an application program execution environment, and interfaces to peripheral devices.

3. **(Original)** The computer, as set forth in claim 1, wherein the computer resource comprises an application program execution environment and a networking system under the control of the operating system and monitored by the intrusion detection system to detect, prevent and report intrusion attempts.

4. **(Original)** The computer, as set forth in claim 1, further comprising an anti-virus system integrated with the operating system and operable to monitor the data storage system, input/output system, networking system, application program execution environment, and interfaces to peripheral devices to detect the presence of at least one virus.

5. **(Original)** The computer, as set forth in claim 1, further comprising an anti-virus system integrated with the operating system and operable to monitor the data storage system, input/output system, networking system, application program execution environment, and interfaces to peripheral devices to detect and report the presence of at least one virus.

6. **(Original)** The computer, as set forth in claim 2, wherein intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames.

7. **(Original)** The computer, as set forth in claim 2, wherein the intrusion detection system is integrated with a networking stack of the networking system above the network layer operable to access reassembled fragments.

8. **(Original)** The computer, as set forth in claim 2, wherein the intrusion detection system is integrated with a networking protocol stack of the networking system above the transport layer.

9. **(Original)** The computer, as set forth in claim 2, wherein the intrusion detection system is integrated with a networking stack of the networking system between the network layer and the transport layer and between the transport layer and the application layer.

10. **(Original)** The computer, as set forth in claim 5, wherein the anti-virus system comprises a module operable to prevent reassembly of a virus.

11. **(Original)** The computer, as set forth in claim 5, wherein the anti-virus system comprises a module operable to recognize a virus.

12. **(Original)** The computer, as set forth in claim 5, wherein the anti-virus system comprises a module operable to prevent storage of a virus.

13. **(Original)** The computer, as set forth in claim 5, wherein the anti-virus system comprises a module operable to prevent transmission of a virus.

14. **(Currently Amended)** The computer, as set forth in claim [[2]] 5, wherein the anti-virus system comprises a module operable to prevent execution of a virus.

15. **(Original)** A method comprising:
executing an OS-integrated intrusion detection system; and
monitoring at least one computer resource to detect and prevent intrusion attempts.

16. **(Original)** The method, as set forth in claim 15, wherein monitoring at least one computer resource comprises monitoring at least one computer resource selected from the group consisting of a data storage system, an input/output system, a networking system, an application program execution environment, and interfaces to peripheral devices.

17. **(Original)** The method, as set forth in claim 15, wherein monitoring at least one computer resource comprises reporting intrusion attempts.

18. **(Original)** The method, as set forth in claim 16, further comprising integrating the intrusion detection system with a networking system above the link layer operable to access raw network frames.

19. **(Original)** The method, as set forth in claim 15, further comprising integrating the intrusion detection system with a networking stack of the networking system above the network layer operable to access reassembled fragments.

20. **(Original)** The method, as set forth in claim 15, further comprising integrating the intrusion detection system with a networking protocol stack of the networking system above the transport layer.

21. **(Original)** The method, as set forth in claim 15, further comprising integrating the intrusion detection system with a networking stack of the networking system between the network layer and the transport layer, and between the transport layer and the application layer.

22. **(Original)** A method comprising:

executing an OS-integrated anti-virus system; and

monitoring at least one computer resource to detect the presence of at least one virus.

23. **(Original)** The method, as set forth in claim 22, wherein monitoring at least one computer resource comprises monitoring at least one computer resource selected from the group consisting of a data storage system, an input/output system, a networking system, an application program execution environment, and interfaces to peripheral devices.

24. **(Original)** The method, as set forth in claim 22, wherein monitoring at least one computer resource comprises reporting the presence of at least one virus.

25. **(Original)** The method, as set forth in claim 22, wherein the step of monitoring comprises detecting the reassembly of a virus.

26. **(Original)** The method, as set forth in claim 22, wherein the step of monitoring comprises recognizing a virus.

27. **(Original)** The method, as set forth in claim 22, wherein the step of monitoring comprises preventing the storage of a virus.

28. **(Original)** The method, as set forth in claim 22, wherein the step of monitoring comprises preventing the transmission of a virus.

29. **(Original)** The method, as set forth in claim 22, wherein the step of monitoring comprises preventing the execution of a virus.